ABSTRACT OF THE DISCLOSURE

A power-residue calculating unit includes a K register connected to a first internal bus for once storing an intermediate calculation result to be discarded when a power-residue calculation is executed in accordance with a binary method. Therefore even when data to be discarded appears during the calculation, a write into K register is performed, so that current in a write operation flows thereby improving immunity against Power Analysis.